7 BEWÄHRTE METHODEN FÜR CYBERSECURITY

An Axis company

DIE SOFTWARE AUF DEM NEUSTEN STAND HALTEN

Die Geräte mit den neuesten Versionen der Firmware auszustatten, ist unabdingbar, wenn Sie mögliche Risiken für die Cybersicherheit verringern wollen. Sobald ein Hersteller eine potenzielle Sicherheitslücke ausfindig macht, schließt er sie über sein anschließendes Software-Update. **Die Installation der Software-Updates sogt dafür, dass Sie die Sicherheitspatches für alle auch erst gerade entdeckten Bedrohungen verwenden.**

2N
An Axis company

STARKE PASSWÖRTER BENUTZEN

Das Mindeste, was Sie als Nutzer tun können, ist die Nutzung eines komplexen Passworts, das nicht so leicht gehackt werden kann. Ideale Passwörter sollten aus mindestens sechs Zeichen bestehen. Es sollte Zahlen, Buchstaben und Symbole miteinander kombinieren. Keine gute Taktik ist es, einfach zu erratende Passwörter wie das Geburtsdatum oder die Heimatstadt zu verwenden. Wenn Sie ein starkes Passwort gefunden haben, vermeiden Sie, dieses nun mit anderen Nutzern zu teilen. Und selbst, wenn Sie alle diese Regeln beachtet haben, ist es ratsam, **Ihr Passwort immer mal wieder zu ändern.**

2N
An Axis company

UNTERSCHIEDLICHE ACCOUNTS FÜR UNTERSCHIEDLICHE ROLLEN

Es ist wichtig, mehrere **Accounts mit unterschiedlichen Zugangsrechten zu unterhalten.** Einem Nutzer wird entsprechend seiner Aufgabe jeweils nur eine begrenzte Möglichkeit zu bestimmten Änderungen eingeräumt. Einmal mehr gilt selbst für diese Accounts: Teilen Sie niemals Ihr Passwort mit anderen Personen. So minimieren Sie die Gefahr, dass sich Ihre Zugangsberechtigungen im Unternehmen verbreiten.

2N
An Axis company

INTERNETANWENDUNGEN BEGRENZEN

Um Schadsoftware zu vermeiden, nutzen Sie **routerbasierte Firewalls,** die verdächtigen Netzverkehr unterbinden, bevor sie auf das Netzwerk übergreifen. Natürlich ist es unmöglich, sich komplett vom Internet abzukoppeln. Aber es ist wichtig, vorsichtig zu sein und das Netzwerk mit starken Passwörtern zu schützen. Angreifer durchforsten das Internet ständig, um miteinander verbundene Geräte ausfindig zu machen. Wenn Sie wissen wollen, welche Geräte Ihres Netzwerks angreifbar sind, können Sie dies auf der Website www.shodan.io selbst herausfinden. Je mehr Geräte Sie von einer direkten Internetnutzung abkoppeln, desto geringer wird das Risiko. Lassen Sie also **nur die jeweils notwendigen Produktfunktionen** eingeschaltet.

2N
An Axis company

DAS NETZWERK SICHERN

a) **Erstellen Sie ein unabhängiges Netzwerk,** das einzig und allein den Geräten dient, die mit sensiblen Informationen umgehen. Durch getrennte Switche können Sie verhindern, dass andere in das Netzwerk eindringen.

b) Nutzen Sie virtuelle **LANs (VLAN).** VLAN verfügt innerhalb eines Datenzentrums über isolierte Netzwerke, und jedes Netzwerk ist eine getrennte Broadcast-Domäne.

c) Sehr nützlich ist ebenfalls die Sicherung des Netzwerkes mit dem **IEEE 802.1X-Protokoll.** Es verhindert den Zugang unautorisierter Geräte in das lokale Netzwerk.

d) Stellen Sie sicher, dass die Hersteller von Geräten und Software, die Sie nutzen, **Protokolle wie HTTPS, TLS, SIPS oder SRTP** ausführen und standardmäßig aktivieren. Das verhindert sogenannte “Man- in-the-Middle”-Cyberangriffe, die von einem dritten Host aus erfolgen können.

2N
An Axis company

DEN RICHTIGEN PROVIDER FÜR DIE FERNSTEUERUNG AUSWÄHLEN

Es ist sehr hilfreich, alle **Installationsstandorte von einem einzigen Account aus zu steuern.** Egal, wo sich der Installationsstandort befindet, so können Sie sie bequem vom Büro aus fernbedienen. Das erscheint als Risiko, wenn Sie an all die oben beschriebenen Gefahren für die Geräte durch das Internet denken. Wählen Sie deshalb einen Provider für die Fernsteuerung, dessen Service auf gesicherten Clouds basiert. Ist das der Fall, müssen Sie sich **nicht mehr mit routerbasierten Firewalls oder Tunneling beschäftigen. Der cloudbasierte Service wird von sich aus eine verschlüsselte Kommunikation sicherstellen.**

2N
An Axis company

DAS IOT-UMFELD SICHERN

Schaffen Sie ein getrenntes **Netzwerk for IoT-Geräte;** wählen Sie ein **starkes Router-Passwort,** um das Netzwerk zu schützen; **installieren Sie niemals neue Elektronik, ohne den Hersteller geprüft zu haben;** lassen Sie keine unnötigen Funktionen auf dem Gerät laufen und bringen Sie die **Firmware und Software** durch fortlaufende Updates auf den neusten Stand.

2N
An Axis company